UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF GEORGIA

TEAIRRA PURVIS, individually, and on behalf of her minor child, J.A., and ARAMAH JOHNSON, and on behalf of all others similarly situated,	)	Case No. 1:20-CV-02277 (LMM)
Plaintiffs,	)	**SECOND AMENDED CLASS ACTION COMPLAINT**
vs.	)	JURY TRIAL DEMANDED
AVEANNA HEALTHCARE, LLC,	)	
Defendant.	)	

SECOND AMENDED CLASS ACTION COMPLAINT

1. Plaintiffs TEAIRRA PURVIS, J.A. (a minor) and ARAMAH JOHNSON, individually, and on behalf of all others similarly situated ("Plaintiffs"), bring this action against Defendant AVEANNA HEALTHCARE, LLC ("AVEANNA" or "Defendant") to obtain damages, restitution, and injunctive relief for the Class, as defined below, from Defendant. Plaintiffs make the following allegations upon information and belief, except as to their own actions, the investigation of their counsel, and the facts that are a matter of public record.

JURISDICTION AND VENUE

2. This Court has jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d) ("CAFA"). There are at least 100 members in the

proposed Class, the aggregated claims of the individual Class Members exceed the sum or value of $5,000,000.00 exclusive of interest and costs, and members of the Proposed Class (such as named Plaintiffs) are citizens of states different from Defendant.

3. Also, this Court has federal question subject matter jurisdiction over this action pursuant to 28 U.S.C. § 1331 because the Plaintiffs assert claims that necessarily raise substantial disputed federal issues under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") and the Federal Trade Commission Act, 15 U.S.C. § 45.

4. Defendant has sufficient minimum contacts in Georgia, as it conducts the majority (if not all) of its business in the State of Georgia, thus rendering the exercise of jurisdiction by this Court proper and necessary.

5. Venue is proper in this District under 28 U.S.C. § 1391 because a substantial part of the events and omissions giving rise to these claims occurred in this District.

NATURE OF THE ACTION

6. This class action arises out of a July 2019 cyberattack and data breach ("Data Breach") at AVEANNA's medical facilities. As a result of the Data Breach, Plaintiffs and approximately 166,077 Class Members suffered ascertainable losses in the form of identity theft and fraud, the loss of the benefit of their bargain, out-of-

pocket expenses, and the value of their time reasonably incurred to remedy or mitigate the effects of the attack. In addition, Plaintiffs and Class Members' sensitive personal information—which was entrusted to AVEANNA, its officials, and agents—was compromised and unlawfully accessed due to the Data Breach. Information compromised in the Data Breach includes social security numbers, dates of birth, bank account and credit card details, passport numbers, driver's licenses, medical record numbers, patient account numbers, diagnosis information, treatment type, and other protected health information as defined by the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), and additional personally identifiable information ("PII") and protected health information ("PHI") that AVEANNA collected and maintained (collectively the "Private Information").

7. Plaintiffs bring this class action lawsuit on behalf of those similarly situated to address Defendant's inadequate safeguarding of Plaintiffs and Class Members' Private Information that Defendant collected and maintained, and for failing to provide timely and adequate notice to Plaintiffs and other Class Members that their Private Information had been subject to the unauthorized access of an unknown third party and precisely what specific Private Information was accessed.

8. Defendant maintained the Private Information in a reckless manner. In particular, the Private Information was maintained on AVEANNA's computer network in a condition vulnerable to cyberattacks, including the infiltration of certain

AVEANNA email accounts containing Plaintiffs and Class Members' Private Information. Upon information and belief, the mechanism of the cyberattack and potential for improper disclosure of Plaintiffs and Class Members' Private Information was a known risk to Defendant, and thus Defendant was on notice that failing to take steps necessary to secure the Private Information from those risks left that property in a dangerous condition.

9. In addition, AVEANNA and its employees failed to properly monitor the computer network and systems that housed the Private Information. Had AVEANNA properly monitored the aforementioned network and systems, it would have discovered the intrusion sooner.

10. Plaintiffs and Class Members' identities are now at risk of compromise because of Defendant's negligent conduct since the Private Information that AVEANNA collected and negligently maintained is now in the hands of data thieves.

11. Armed with the Private Information accessed in the Data Breach, data thieves can and have committed a variety of crimes including, by way of non-exhaustive examples: opening new financial accounts in Class Members' names (including financial accounts in Plaintiff Johnson's name); taking out loans in Class Members' names; using Class Members' names to obtain medical services; using Class Members' health information to target other phishing and hacking intrusions

based on their individual health needs; using Class Members' information to obtain government benefits; filing fraudulent tax returns using Class Members' information; obtaining driver's licenses in Class Members' names but with another person's photograph; and giving false information to police during an arrest.

12. As a result of the Data Breach, Plaintiffs and Class Members have been exposed to a heightened and imminent risk of fraud and identity theft, and, in fact, have been the victims of fraud and identity theft. Plaintiffs and Class Members must now and in the future closely monitor their financial accounts, credit reports, tax returns, and similar, otherwise secure accounts to guard against identity theft.

13. Plaintiffs and Class Members may also incur out-of-pocket costs for, by way of non-exhaustive examples: purchasing credit monitoring services; credit freezes; credit reports; or other protective measures to deter and detect identity theft.

14. By their Complaint, Plaintiffs seek to remedy these harms on behalf of themselves and all similarly situated individuals whose Private Information was accessed during the Data Breach.

15. Plaintiffs seek remedies including, but not limited to, nominal damages, compensatory damages, reimbursement of out-of-pocket costs, the cost of identity theft protection, and injunctive relief including improvements to Defendant's data security systems, future annual audits, and funded by Defendant.

16. Accordingly, Plaintiffs bring this action against Defendant seeking redress for its unlawful conduct, and asserting claims for: (i) negligence; (ii) intrusion into private affairs; (iii) negligence *per se*; (iv) breach of express contract; (v) breach of implied contract; (vi) breach of fiduciary duty; and (vii) breach of confidence.

PARTIES

17. Plaintiff TEAIRRA PURVIS is, and at all times mentioned herein was, an individual citizen of the state of Georgia residing in the City of Decatur.

18. Plaintiff J.A. is, and at all times mentioned herein was, an individual citizen of the state of Georgia residing in the City of Decatur.

19. Plaintiff ARAMAH JOHNSON is, and at all times mentioned herein was, an individual citizen of the State of Maryland residing in the City of Baltimore.

20. Defendant AVEANNA is a corporation organized under the laws of the state of Delaware with its principal place of business in Atlanta, Georgia.

DEFENDANT'S BUSINESS

21. AVEANNA is the nation's largest provider of pediatric home care. It offers pediatric nursing, pediatric therapy, autism services, enteral nutrition, therapy, and adult services.

22. AVEANNA was formed after two of the largest providers of pediatric care in the nation—Epic Health Services and PSA Healthcare—were merged.

23. Today, AVEANNA cares for patients in twenty-three (23) states through its network of more than 200 branch offices.

24. According to AVEANNA, its broad range of services expands beyond in-home private duty nursing care to include in-home aide services, respite care, school nurse services, therapies, and rehabilitation.

25. In the ordinary course of receiving treatment and health care services from AVEANNA, patients and their families are required to provide Defendant with sensitive, personal, and private information such as:

- Name, address, phone number and email address;
- Date of birth;
- Demographic information;
- Social Security number;
- Information relating to individual medical history;
- Insurance information and coverage;
- Information concerning an individual's doctor, nurse, or other medical providers;
- Photo identification;
- Employer information; and
- Other information that may be deemed necessary to provide care.

26. AVEANNA also gathers certain medical information about patients and creates records of the care it provides to them.

27. Additionally, AVEANNA may receive private and personal information from other individuals and/or organizations that are part of a patient's "circle of care," such as referring physicians, patients' other doctors, patients' health plan(s), close friends, and/or family members.

28. All of Defendant's employees, staff, entities, clinics, sites, and locations may share patient information with each other for various purposes without a written authorization, as disclosed in AVEANNA's Joint Notice of Privacy Practices (the "Privacy Notice").[1] The current Privacy Notice has an effective date of January 2003 and most recently revised date of January 2014.

29. The Privacy Notice is provided to every patient upon request and is posted on Defendant's website.

30. Because of the highly sensitive and personal nature of the information Defendant acquires and stores with respect to its patients, AVEANNA promises to, among other things: (i) "[m]aintain the privacy of protected health information;" (ii) "[p]rovide you with this notice of its legal duties and privacy practices with respect to your protected health information;" (iii) "[n]otify you following a breach of

[1] https://www.aveanna.com/privacyhipaa/.

unsecured protected health information;" (iv) [a]bide by the terms of this notice; and (v) "[o]btain your written authorization to use or disclose your health information for reasons other than those listed above and permitted under law."[2]

31. In the course of treating patients, Defendant acquires, collects, and stores a massive amount of personally identifiable information on its patients.

32. As a condition of receiving medical care and treatment from Defendant, Defendant requires that its patients entrust it with highly sensitive personal information.

33. In the ordinary course of providing treatment and health care services, AVEANNA employs hundreds of persons nationwide, including nurses, nursing assistants, physical and occupational therapists, direct support professionals, pediatric care providers, companion and personal care employees, and administrative personnel.

34. As a condition of employment, AVEANNA requires that its employees and contractors entrust it with highly sensitive personal information, including names, addresses, phone numbers, email addresses, Social Security numbers, driver's licenses or other forms of identification that will satisfy the I-9 form

[2] *Id.*

requirement, photo identification, work history (including dates of prior employment), direct deposit banking information, and other PII.

35. In the course of employment, AVEANNA creates PII for its employees, including (among other things) unique employee identification numbers.

36. AVEANNA employees and contractors work pursuant to employment contracts.

37. By obtaining, collecting, using, and deriving a benefit from Plaintiffs and Class Members' PII, Defendant assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiffs and Class Members' PII from disclosure.

38. Plaintiffs and the Class Members have taken reasonable steps to maintain the confidentiality of their PII.

39. Plaintiffs and the Class Members relied on Defendant to keep their PII confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information.

PLAINTIFFS' EXPERIENCES

40. Plaintiff Purvis is the mother of Plaintiff J.A., a minor, and is the financially responsible party for Plaintiff J.A.'s medical care and treatment.

41. Plaintiff J.A. was a patient of and received medical services from Defendant beginning in 2018.

42. On the first occasion(s) in 2018 on which Plaintiff J.A. received medical care and treatment from Defendant (the exact dates of which are known to Defendant through its own records), Plaintiff Purvis provided Defendant with her and her child Plaintiff J.A.'s name; her address, phone number and email address; the date of birth of Plaintiff J.A.; their demographic information (race, gender, etc.); their Social Security numbers; information relating to Plaintiff J.A.'s individual medical history; insurance information and coverage, Medicaid information, and information about her employer (the Board of Education).

43. Plaintiff Purvis was required to provide this information to Defendant as a condition of Plaintiff J.A. receiving medical care and treatment from Defendant.

44. In the course of treating Plaintiff J.A., a minor, Defendant produced PII and PHI for J.A., including a medical record number, patient account number, diagnosis information, records of treatment (including doctor names), billing/claims information, and prescription/medication information and name.

45. In the course of treating Plaintiff J.A., a minor, Defendant also produced PHI containing Plaintiff J.A.'s date of birth, and health insurance number/other health insurance information.

46. Plaintiff Johnson was an employee or contractor of AVEANNA and its predecessor entities. Plaintiff Johnson initially started working for AVEANNA (via one of its predecessor entities or acquired companies—Clarity Service Group) in

August 2014, and worked for Clarity Service Group until June 2015. She was rehired by AVEANNA (via another predecessor entity or acquired company—Epic Developmental Services) in December 2015. Epic Developmental Systems merged, and the merged entity became AVEANNA in the summer of 2019, and Plaintiff Johnson continued her employment with AVEANNA until March 12, 2020, when she was laid off due to COVID-19.

47. At the time she applied for employment with Clarity Service Group in or about August 2014 (the exact date of which is known to Defendant through its own records), Plaintiff Johnson was required to and did provide Defendant (or its predecessor or acquired entity) with her name; her address, phone number and email address; her date of birth; her Social Security number, and direct deposit banking information.

48. Plaintiff Johnson was required to and did provide this information to Defendant as a condition of Plaintiff Johnson applying for and obtaining employment with Defendant (or its predecessor/acquired entity). Upon information and belief, all PII provided to any predecessor company or acquired entity was transferred to and came into the possession of AVEANNA.

49. Plaintiff Johnson entered into an employment contract with Defendant, a material term of which was that Defendant agreed to keep Plaintiff Johnson's PII and other personal information safe and confidential.

THE CYBERATTACK AND DATA BREACH

50. In July 2019, a cyberattack against AVEANNA occurred that involved some of its patients' Private Information that was contained in email accounts of AVEANNA employees.[3]

51. Those employee email accounts were compromised by data thieves, utilizing "phishing" techniques.

52. The phishing cyberattack was targeted at Defendant due to Defendant's status as a healthcare entity that collects, creates, and maintains both PII and PHI. The targeted phishing cyberattack was expressly designed to gain access to private and confidential data, including (among other things) the PII and PHI of patients like Plaintiffs and Class Members.

53. AVEANNA became aware of the incident on or about August 24, 2019.

54. Upon learning of the incident, AVEANNA initiated a security incident investigation to determine the nature and scope of the cyberattack.

55. The investigation determined that an unknown intruder accessed certain employee email accounts between July 9, 2019 and August 24, 2019.

56. AVEANNA determined that the compromised employee email accounts contained Private Information belonging to patients like Plaintiffs and

[3] https://www.aveanna.com/data-privacy-event/.

Class Members, including Social Security numbers, dates of birth, employee identification numbers, bank/financial account numbers, credit/debit card numbers with CVV and expiration date, passport numbers, driver's license numbers, usernames and passwords, medical record numbers, patient account numbers, diagnosis information, treatment type and location, doctor names, health insurance information, billing/claims information, Medicare/Medicaid ID numbers, and prescription/medication information.

57. Plaintiff Purvis was sent a Notice of Data Breach letter, attached hereto as Exhibit A. The notice informed Plaintiff Purvis of the Data Breach, and stated that the email accounts that were compromised in the Data Breach contained her date of birth, driver's license/state ID and name. *See* Exhibit A.

58. Based upon the Data Breach notice that she received, and based upon the information that she entrusted to Defendant, Plaintiff Purvis believes her Private Information was stolen (and subsequently sold) in the Data Breach.

59. Plaintiff Purvis also received a separate Notice of Data Breach letter for her child, Plaintiff J.A. A redacted copy of this letter, dated February 14, 2020, is attached hereto as Exhibit B.

60. The Data Breach notice letter relating to Plaintiff J.A. informed the parent or guardian of J.A., a minor, of the Data Breach, and stated that the email

accounts that were compromised in the Data Breach contained the following types of Plaintiff J.A.'s personal information:

> date of birth, medical record number, patient account number, diagnosis information, treatment type or location, doctor name, health insurance number/other health insurance information, billing/claims information, Medicare/Medicaid ID and prescription/medication information and name.

See Exhibit B.

61. The Data Breach notice letter sent to Plaintiff Purvis as the parent and guardian of Plaintiff J.A. offered Plaintiff J.A. access to twelve (12) months of child identity protection services from Equifax at no cost to Plaintiffs. *See* Exhibit B.

62. Defendant's offer of identity protection services to Plaintiff J.A. acknowledges that the risk of future injury is actual, choate, imminent and certainly impending.

63. Based upon the Data Breach notice sent to the parent or guardian of Plaintiff J.A., the information about Plaintiff J.A. entrusted to Defendant, the protected health information created by Defendant in the course of treating Plaintiff J.A., the Data Breach notice letter sent to Plaintiff J.A., and the offer of child identity protection services made to Plaintiff J.A., Plaintiffs believe Plaintiff J.A.'s Private Information was stolen (and subsequently sold) in the Data Breach.

64. Plaintiff Johnson was sent a Notice of Data Breach letter, attached hereto as Exhibit C. The notice informed Plaintiff Johnson of the Data Breach, and

stated that the email accounts that were compromised in the Data Breach contained her Social Security number, date of birth, employee identification number and name. *See* Exhibit C.

65. The Data Breach notice letter sent to Plaintiff Johnson offered Plaintiff Johnson access to twelve (12) months of identity protection services from TransUnion at no cost to Plaintiff Johnson. *See* Exhibit C.

66. On July 28, 2020, Equifax registered a "soft inquiry" from SunTrust Bank in Southwest Florida.

67. On that same date or shortly thereafter, an unknown person or unknown persons went online and opened two banking accounts (an "Essential Checking" account and an "Essential Savings" account) in Plaintiff Johnson's name with SunTrust Bank.

68. Plaintiff Johnson did not open these banking accounts, and did not authorize any other person to open these banking accounts in her name.

69. On August 3, 2020, an unknown person or unknown persons initiated and completed an address change for the newly created SunTrust Bank accounts, changing the address from Ms. Johnson's home address in Baltimore, Maryland to an address in New Palestine, Indiana.

70. Plaintiff Johnson is not connected in any way with any address in the State of Indiana, including the address in New Palestine, Indiana provided to

SunTrust Bank as part of the address change initiated and completed by unknown person(s).

71. On August 10, 2020, an unknown person(s) initiated and completed two one-cent ACH transactions (one credit and one debit transaction) on one of the two newly opened accounts.

72. Plaintiff Johnson only became aware of the creation of the two SunTrust Bank accounts opened in her name when she received two welcome letters (one for each account) from SunTrust on or about August 10, 2020. The two letters were sent to Plaintiff Johnson's home address in Baltimore, Maryland.

73. Plaintiff Johnson was also mailed printed checks and deposit slips bearing Plaintiff Johnson's name and Baltimore, Maryland address. These checks would have ended up in the hands of unknown person(s), if the address change initiated by unknown person(s) had been processed by SunTrust Bank prior to generating the welcome letters, checks, and deposit slips.

74. Upon receiving the two welcome letters, Plaintiff Johnson immediately contacted SunTrust Bank, letting it know that she did not open any accounts with it. SunTrust took her information and told her that it would be commencing an investigation.

75. After spending time on the phone with SunTrust, Plaintiff Johnson next spent time going to a SunTrust Bank physical branch to try and find out more

information about these fraudulent bank accounts, was told that the accounts were opened online, and was told that anyone could open an account in her name if they had her private information.

76. Plaintiff Johnson then contacted all three credit bureaus to put a fraud alert on her credit report, and initiated a security freeze, expending additional time and effort dealing with the identity theft and fraud.

77. To the best of her knowledge and belief, Plaintiff Johnson is unaware of any other incident involving any other company or business entity in which her PII has been compromised by cyberthieves, and has never previously been the victim of identity theft or fraud related to identity theft (aside from the Data Breach).

78. Based upon the Data Breach notice that she received, based upon the information that she entrusted to Defendant, and based upon the actual identity theft and fraud perpetrated against her, Plaintiff Johnson believes her Private Information was stolen in the Data Breach.

79. All forms of the Data Breach Notice letter indicate that AVEANNA has been unable to rule out if Private Information was stolen in the Data Breach, and instead note (for example) that the investigation into the Data Breach "was not able to determine whether your minor's information was actually viewed or taken by the unauthorized intruder." *See* Exhibit B; *see also* Exhibits A and C.

80. Despite being unable to rule out that the Private Information of Plaintiffs and the Class Members was not compromised, AVEANNA did not begin to notify affected employees until February 14, 2020, and potentially affected patients until February 18, 2020, nearly six (6) months after the Data Breach was first discovered in August 2019.

81. Defendant had obligations created by HIPAA, contract, industry standards, common law, and representations made to Plaintiffs and Class Members, to keep their Private Information confidential and to protect it from unauthorized access and disclosure.

82. Plaintiffs and Class Members provided their Private Information to Defendant with the reasonable expectation and mutual understanding that Defendant would comply with its obligations to keep such information confidential and secure from unauthorized access.

83. Defendant's data security obligations were particularly important given the substantial increase in cyberattacks and data breaches in the healthcare industry preceding the date of the Data Breach.

84. Indeed, cyberattacks have become so notorious that the Federal Bureau of Investigation ("FBI") and United States Secret Service have issued a warning to potential targets, so they are aware of, and prepared for, a potential attack. As one report explained, "[e]ntities like smaller municipalities and ***hospitals*** are attractive

to ransomware criminals . . . because they often have lesser IT defenses and a high incentive to regain access to their data quickly."[4]

85. Therefore, the increase in such attacks, and attendant risk of future attacks, was widely known to the public and to anyone in Defendant's industry, including AVEANNA.

86. Phishing attacks of the type that the unauthorized persons used to gain access to Defendant's employee email accounts are among the oldest, most common, and well-known form of cyberattacks. "Phishing is a cyberattack that uses disguised email as a weapon. The goal is to trick the email recipient into believing that the message is something they want or need—a request from their bank, for instance, or a note from someone in their company—and to click a link or download an attachment."[5] The fake link will typically mimic a familiar website and require the input of credentials. Once inputted, the credentials are then used to gain unauthorized access into a system. "It's one of the oldest types of cyber-attacks, dating back to the 1990s" and one that every organization with an internet presence is aware."[6] It

[4] https://www.law360.com/consumerprotection/articles/1220974/fbi-secret-service-warn-oftargeted-ransomware?nlpk=3ed44a08-fcc2-4b6c-89f0aa0155a8bb51&utmsource=newsletter&utmmedium=email&utm_campaign=consumerprotection (emphasis added).

[5] Frulingher, J., "What is phishing? How this cyber-attack works and how to prevent it," CSO Online, Apr. 7, 2020, https://www.csoonline.com/article/2117843/what-is-phishing-how-this-cyber-attack-works-and-how-to-prevent-it.html (last visited June 20, 2020).

[6] *Id.*

remains the "simplest kind of cyberattack and, at the same time, the most dangerous and effective."[7]

87. Phishing attacks are generally preventable with the implementation of a variety of proactive measures such as purchasing and using some sort of commonly available anti-malware security software (such as the ubiquitous Malwarebites). Most cybersecurity tools have the ability to detect when a link or an attachment isn't what it seems.[8] Other proactive measures include sandboxing inbound e-mail (*i.e.* an automated process that segregates e-mail with attachments and links to an isolated test environment, or a "sandbox," wherein a suspicious file or URL may be executed safely), inspecting and analyzing web traffic, penetration testing (which can be used to test an organization's security policy, its adherence to compliance requirements, its employees' security awareness and the organization's ability to identify and respond to security incidents), and employee education, just to name some of the well-known tools and techniques to prevent phishing attacks.

DEFENDANT FAILS TO COMPLY WITH FTC GUIDELINES

88. The Federal Trade Commission ("FTC") has promulgated numerous guides for businesses which highlight the importance of implementing reasonable

[7] Phishing, Malwarebytes, https://www.malwarebytes.com/phishing/ (last visited June 20, 2020).
[8] *Id.*

data security practices. According to the FTC, the need for data security should be factored into all business decision-making.

89. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established cyber-security guidelines for businesses. The guidelines note that businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.

90. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

91. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ

reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45 ("FTCA"). Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

92. These FTC enforcement actions include actions against healthcare providers like Defendant. *See, e.g.*, *LabMD, Inc., A Corp*, 2016-2 Trade Cas. (CCH) ¶ 79708, 2016 WL 4128215, at *32 (MSNET July 28, 2016) ("[T]he Commission concludes that LabMD's data security practices were unreasonable and constitute an unfair act or practice in violation of Section 5 of the FTC Act.").

93. Defendant failed to properly implement basic data security practices, including failing to implement multifactor authentication. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to patient PII and PHI constitutes an unfair act or practice prohibited by Section 5 of the FTCA, 15 U.S.C. § 45.

94. Defendant was at all times fully aware of its obligation to protect the PII and PHI of its patients. Defendant was also aware of the significant repercussions that would result from its failure to do so.

DEFENDANT FAILS TO COMPLY WITH INDUSTRY STANDARDS

95. As shown above, experts studying cyber security routinely identify healthcare providers as being particularly vulnerable to cyberattacks because of the value of the PII and PHI which they collect and maintain.

96. Several best practices have been identified that a minimum should be implemented by healthcare providers like Defendant, including but not limited to: educating all employees; strong passwords; multi-layer security, including firewalls, anti-virus, and anti-malware software; encryption, making data unreadable without a key; multi-factor authentication; backup data, and; limiting which employees can access sensitive data.

97. A number of industry and national best practices have been published and should be used as a go-to resource when developing an institution's cybersecurity standards. The Center for Internet Security ("CIS") released its Critical Security Controls, and all healthcare institutions are strongly advised to follow these actions. The CIS Benchmarks are the overwhelming option of choice for auditors worldwide when advising organizations on the adoption of a secure build standard for any governance and security initiative, including PCI DSS, HIPAA, NIST 800-53, SOX, FISMA, ISO/IEC 27002, Graham Leach Bliley and ITIL.

98. Other best cybersecurity practices that are standard in the healthcare industry include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches and routers; monitoring and protection of physical security systems; protection against any possible communication system; training staff regarding critical points.

99. Defendant failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework, NIST Special Publications 800-53, 53A, or 800-171; General Accounting Office ("GAO") standards; the Federal Risk and Authorization Management Program ("FEDRAMP"); and the Center for Internet Security's Critical Security Controls ("CIS CSC"), which are all established standards in reasonable cybersecurity readiness.

100. Defendant failed to meet the industry standard of implementing multifactor authentication prior to the Data Breach.

DEFENDANT'S CONDUCT VIOLATED THE STANDARDS MANDATED BY HIPAA REGULATIONS AND DEMONSTRATES ITS INSUFFICIENT DATA SECURITY

101. HIPAA requires covered entities to protect against reasonably anticipated threats to the security of sensitive patient health information.

102. Covered entities must implement safeguards to ensure the confidentiality, integrity, and availability of PHI. Safeguards must include physical, technical, and administrative components.

103. Title II of HIPAA contains what are known as the Administrative Simplification provisions. 42 U.S.C. §§ 1301, *et seq.* These provisions require, among other things, that the Department of Health and Human Services ("HHS") create rules to streamline the standards for handling PII like the data Defendant left unguarded. The HHS subsequently promulgated multiple regulations under authority of the Administrative Simplification provisions of HIPAA. These rules include 45 C.F.R. § 164.306(a)(1-4); 45 C.F.R. § 164.312(a)(1); 45 C.F.R. § 164.308(a)(1)(i); 45 C.F.R. § 164.308(a)(1)(ii)(D), and 45 C.F.R. § 164.530(b).

104. Defendant's Data Breach resulted from a combination of insufficiencies, including without limitation lack of training in the proper handling of phishing emails and the lack of multifactor authentication, that demonstrate they failed to comply with safeguards mandated by HIPAA regulations, and therefore violated the standards embodied in the HIPAA regulations.

DEFENDANT'S BREACH

105. Defendant breached its obligations to Plaintiffs and Class Members and/or was otherwise negligent and reckless because it failed to properly maintain and safeguard its computer systems and data—including Plaintiffs and Class

Members' Private Information. Defendant's unlawful conduct includes, but is not limited to, the following acts and/or omissions:

a. Failing to maintain an adequate data security system to reduce the risk of data breaches and cyberattacks;

b. Failing to adequately protect patients' Private Information;

c. Failing to properly monitor its own data security systems for existing intrusions, brute-force attempts, and clearing of event logs;

d. Failing to implement multifactor authentication;

e. Failing to apply all available security updates;

f. Failing to install the latest software patches, update its firewalls, check user account privileges, or ensure proper security practices;

g. Failing to practice the principle of least-privilege and maintain credential hygiene

h. Failing to avoid the use of domain-wide, admin-level service accounts;

i. Failing to employ or enforce the use of strong randomized, just-in-time local administrator passwords;

j. Failing to properly train and supervise employees in the proper handling of inbound emails;

k. Failing to properly monitor its own data security systems for existing intrusions;

l. Failing to ensure that its vendors with access to its computer systems and data employed reasonable security procedures;

m. Failing to ensure the confidentiality and integrity of electronic PHI it created, received, maintained, and/or transmitted, in violation of 45 C.F.R. § 164.306(a)(1);

n. Failing to implement technical policies and procedures for electronic information systems that maintain electronic PHI to allow access only to those persons or software programs that have been granted access rights in violation of 45 C.F.R. § 164.312(a)(1);

o. Failing to implement policies and procedures to prevent, detect, contain, and correct security violations in violation of 45 C.F.R. § 164.308(a)(1)(i);

p. Failing to implement procedures to review records of information system activity regularly, such as audit logs,

access reports, and security incident tracking reports in violation of 45 C.F.R. § 164.308(a)(1)(ii)(D);

q. Failing to protect against reasonably anticipated threats or hazards to the security or integrity of electronic PHI in violation of 45 C.F.R. § 164.306(a)(2);

r. Failing to protect against reasonably anticipated uses or disclosures of electronic PHI that are not permitted under the privacy rules regarding individually identifiable health information in violation of 45 C.F.R. § 164.306(a)(3);

s. Failing to ensure compliance with HIPAA security standard rules by its workforces in violation of 45 C.F.R. § 164.306(a)(4);

t. Failing to train all members of its workforces effectively on the policies and procedures regarding PHI as necessary and appropriate for the members of its workforces to carry out their functions and to maintain security of PHI, in violation of 45 C.F.R. § 164.530(b); and/or

u. Failing to render the electronic PHI it maintained unusable, unreadable, or indecipherable to unauthorized individuals, as it had not encrypted the electronic PHI as specified in the

> HIPAA Security Rule by "the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key" (45 C.F.R. § 164.304 definition of encryption).

106. As the result of computer systems in dire need of security upgrading, inadequate procedures for handling phishing emails containing viruses or other malignant computer code, and employees who opened files containing the virus or malignant code that perpetrated the cyberattack, Defendant AVEANNA negligently and unlawfully failed to safeguard Plaintiffs and Class Members' Private Information.

107. Accordingly, as outlined below, Plaintiffs and Class Members' daily lives were severely disrupted. What's more, they now face an increased risk of fraud and identity theft. Plaintiffs and the Class Members also lost the benefit of the bargain they made with Defendant.

PREVALENCE OF CYBER ATTACKS AND SUSCEPTIBILITY OF THE HEALHCARE SECTOR

108. Data breaches, including those perpetrated against the healthcare sector of the economy, have become widespread. In 2016, the number of U.S. data breaches surpassed 1,000, a record high and a forty percent increase in the number of data

breaches from the previous year. In 2017, a new record high of 1,579 breaches were reported, representing a 44.7 percent increase over 2016. In 2018, there was an extreme jump of 126 percent in the number of consumer records exposed from data breaches. In 2019, there was a 17 percent increase in the number of breaches (1,473) over 2018, with 164,683,455 sensitive records exposed.

109. The number of data breaches in the healthcare sector skyrocketed in 2019, with 525 reported breaches exposing nearly 40 million sensitive records (39,378,157), compared to only 369 breaches that exposed just over 10 million sensitive records (10,632,600) in 2018.[9]

110. Phishing cyberattacks against healthcare organizations are targeted. According to the 2019 Health Information Management Systems Society, Inc. ("HIMMS") Cybersecurity Survey, "[a] pattern of cybersecurity threats and experiences is discernable across US healthcare organizations. Significant security incidents are a near-universal experience in US healthcare organizations with many of the incidents initiated by bad actors, leveraging e-mail as a means to compromise the integrity of their targets."[10] "Hospitals have emerged as a primary target because they sit on a gold mine of sensitive personally identifiable information for thousands of patients at any given time. From Social Security and insurance policies to next of

[9] https://www.idtheftcenter.org/wp-content/uploads/2020/01/01.28.2020_ITRC_2019-End-ofYear-Data-Breach-Report_FINAL_Highres-Appendix.pdf
[10] https://www.himss.org/himss-cybersecurity-survey (last accessed June 20, 2020).

kin and credit cards, no other organization, including credit bureaus, have so much monetizable information stored in their data centers."[11]

111. The exposure of highly personal and highly confidential healthcare related data is of great consequence to patients. As the ID Theft Center notes:

> Medical identity theft is costly to consumers. Unlike credit-card fraud, victims of medical identity theft can suffer significant financial consequences. Sixty-five percent of medical identity theft victims had to pay an average of $13,500 to resolve the crime. In some cases, they paid the health care provider, repaid the insurer for services obtained by the thief, or they engaged an identity-service provider or legal counsel to help resolve the incident and prevent fraud.
>
> Those who have resolved the crime spent, on average, more than 200 hours on such activities as working with their insurer or health-care provider.
>
> Medical identity theft can have a negative impact on reputation. Forty-five percent of respondents said medical identity theft affected their reputation mainly because of embarrassment due to disclosure of sensitive personal health conditions; 19 percent of respondents believed the theft caused them to miss out on career opportunities. Three percent said it resulted in the loss of employment.[12]

[11] https://www.idigitalhealth.com/news/how-to-safeguard-hospital-data-from-email-spoofing-attacks (last accessed June 20, 2020).
[12] https://www.idtheftcenter.org/medical-id-theft-costs-victims-big-money/#:~:text=Medical%20identity%20theft%20is%20costly,%2413%2C500%20to%20resolve%20the%20crime (last accessed June 20, 2020).

CYBERATTACKS AND DATA BREACHES CAUSE DISRUPTION AND PUT CONSUMERS AT AN INCREASED RISK OF FRAUD AND IDENTIFY THEFT

112. Cyberattacks and data breaches at medical facilities like AVEANNA are especially problematic because of the disruption they cause to the medical treatment and overall daily lives of patients affected by the attack.

113. Researchers have found that at medical facilities that experienced a data security incident, the death rate among patients increased in the months and years after the attack.[13]

114. Researchers have found that at medical facilities that experienced a data security incident, the death rate among patients increased in the months and years after the attack.[14]

115. Researchers have further found that at medical facilities that experienced a data security incident, the incident was associated with deterioration in timeliness and patient outcomes, generally.[15]

116. Cyberattacks such as one at issue here are considered a breach under the HIPAA Rules because there is an access of PHI not permitted under the HIPAA Privacy Rule:

---

[13] *See* https://www.pbs.org/newshour/science/ransomware-and-other-data-breaches-linked-to-uptick-in-fatal-heart-attacks
[14] *See* https://www.pbs.org/newshour/science/ransomware-and-other-data-breaches-linked-to-uptick-in-fatal-heart-attacks
[15] *See* https://onlinelibrary.wiley.com/doi/full/10.1111/1475-6773.13203.

> A breach under the HIPAA Rules is defined as, " . . . the acquisition, access, use, or disclosure of PHI in a manner not permitted under the [HIPAA Privacy Rule] which compromises the security or privacy of the PHI." *See* 45 C.F.R. 164.40.[16]

117. The United States Government Accountability Office released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[17]

118. The FTC recommends that identity theft victims take several steps to protect their personal and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for seven (7) years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.[18]

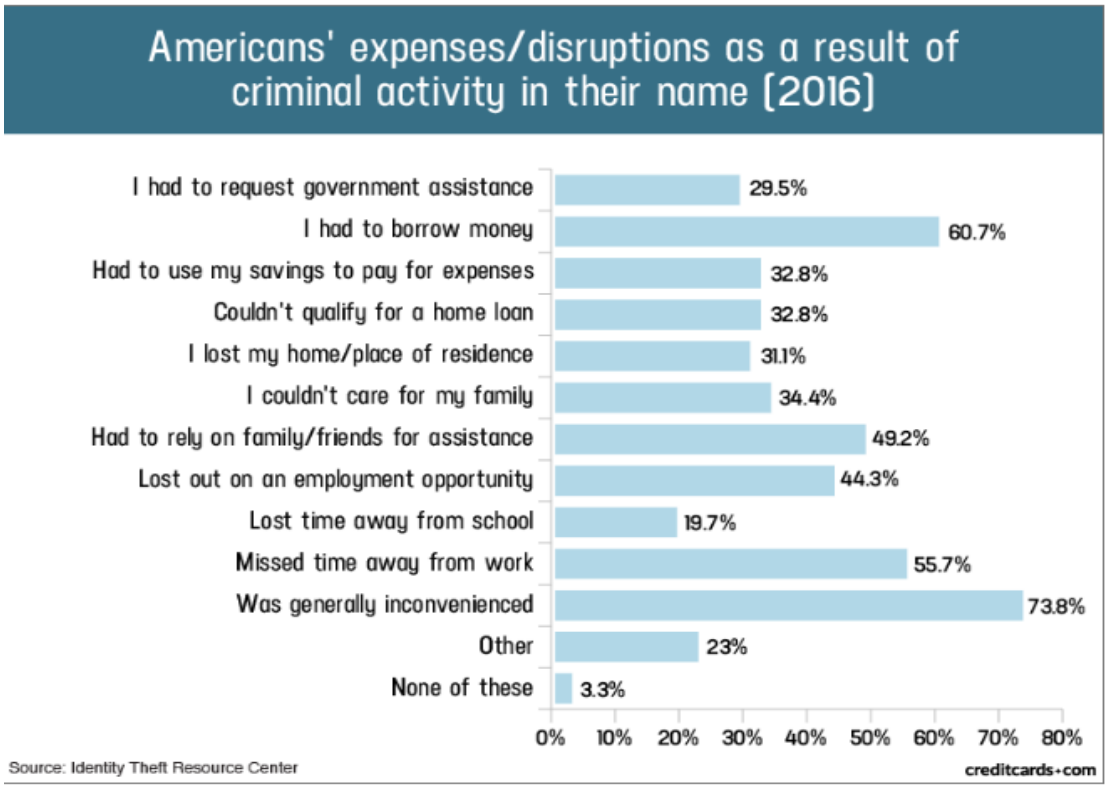
119. Identity thieves use stolen personal information such as Social Security numbers for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.

120. Identity thieves can also use Social Security numbers to obtain a driver's license or official identification card in the victim's name but with the thief's

---

[16] *Id.*
[17] *See* "Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown," p. 2, U.S. Government Accountability Office, June 2007, https://www.gao.gov/new.items/d07737.pdf (last visited Apr. 12, 2019) ("GAO Report").
[18] *See* https://www.identitytheft.gov/Steps (last visited Apr. 12, 2019).

picture; use the victim's name and Social Security number to obtain government benefits; or file a fraudulent tax return using the victim's information. In addition, identity thieves may obtain a job using the victim's Social Security number, rent a house or receive medical services in the victim's name, and may even give the victim's personal information to police during an arrest resulting in an arrest warrant being issued in the victim's name. A study by Identity Theft Resource Center shows the multitude of harms caused by fraudulent use of personal and financial information:[19]



[19] "Credit Card and ID Theft Statistics" by Jason Steele, 10/24/2017, at: https://www.creditcards.com/credit-card-news/credit-card-security-id-theft-fraud-statistics-1276.php (last visited June 20, 2019).

121. What's more, theft of Private Information is also gravely serious. PII/PHI is a valuable property right.[20] Its value is axiomatic, considering the value of Big Data in corporate America and the consequences of cyber thefts include heavy prison sentences. Even this obvious risk to reward analysis illustrates beyond doubt that Private Information has considerable market value.

122. Theft of PHI, in particular, is gravely serious: "A thief may use your name or health insurance numbers to see a doctor, get prescription drugs, file claims with your insurance provider, or get other care. If the thief's health information is mixed with yours, your treatment, insurance and payment records, and credit report may be affected."[21] Drug manufacturers, medical device manufacturers, pharmacies, hospitals and other healthcare service providers often purchase PII/PHI on the black market for the purpose of target marketing their products and services to the physical maladies of the data breach victims themselves. Insurance companies purchase and use wrongfully disclosed PHI to adjust their insureds' medical insurance premiums.

123. It must also be noted there may be a substantial time lag—measured in years—between when harm occurs versus when it is discovered, and also between when Private Information, financial information, and other sensitive data is stolen

[20] *See, e.g.*, John T. Soma, et al, Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets, 15 Rich. J.L. & Tech. 11, at *3-4 (2009) ("PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted).
[21] *See* Federal Trade Commission, Medical Identity Theft, http://www.consumer.ftc.gov/articles/0171-medical-identity-theft (last visited Mar. 27, 2020).

and when it is used (like in the case of Plaintiff Johnson). According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.

See GAO Report at 29.

124. Private Information and financial information are such valuable commodities to identity thieves that once the information has been compromised, criminals often trade the information on the "cyber black-market" for years.

125. There is a strong probability that entire batches of stolen information have been dumped on the black market and are yet to be dumped on the black market, meaning Plaintiffs and Class Members are at an increased risk of fraud and identity theft for many years into the future. Thus, Plaintiffs and Class Members must vigilantly monitor their financial and medical accounts for many years to come.

126. Medical information is especially valuable to identity thieves. According to account monitoring company LogDog, coveted Social Security numbers were selling on the dark web for just $1 in 2016—the same as a Facebook

account. That pales in comparison with the asking price for medical data, which was selling for $50 and up.[22]

127. Because of its value, the medical industry has experienced disproportionally higher numbers of data theft events than other industries. Defendant therefore knew or should have known this and strengthened its network and data systems accordingly. Defendant was put on notice of the substantial and foreseeable risk of harm from a data breach, yet it failed to properly prepare for that risk, resulting in the Data Breach.

PLAINTIFFS AND CLASS MEMBERS' DAMAGES

128. To date, Defendant has done absolutely nothing to provide Plaintiffs and the Class Members with relief for the damages they have suffered as a result of the Data Breach.

129. To date, Defendant has not even offered Plaintiff Purvis and all the Class Members any free credit monitoring, identity theft protection, or identity restoration services.

130. Free credit monitoring was only offered to those whose Social Security numbers were deemed compromised, like Plaintiff Johnson, and to minors like Plaintiff J.A. Even then, the credit monitoring was inadequate, covering only one

[22] https://nakedsecurity.sophos.com/2019/10/03/ransomware-attacks-paralyze-and-sometimescrush-hospitals/#content; https://getlogdog.com/blogdog/email-security-you-are-doing-it-wrong/

year, when the type of fraud and other risks can lag and persist for years, as evidenced by the identity theft and fraud perpetrated against Plaintiff Johnson on or about July 28, 2020, over one year after the Data Breach first began occurring on July 9, 2019.

131. Instead of offering any real assistance or compensation, Defendant actively encouraged Plaintiffs and the Class Members to spend their personal time dealing with the aftereffects of the Data Breach, recommending that Plaintiffs and Class Members take the time to "regularly monitor credit reports, account statements and benefit statements," rather than offering a service to monitor on behalf of Plaintiffs and Class Members.[23]

132. Plaintiffs and Class Members have been damaged by the compromise of their Private Information in the Data Breach.

133. Plaintiffs' PII and PHI was compromised as a direct and proximate result of the Data Breach.

134. As a direct and proximate result of the Data Breach, Plaintiffs' PII and PHI was exfiltrated and is in the hands of identity thieves and criminals, as evidenced by the identity theft and fraud perpetrated against Plaintiff Johnson described above.

[23] https://www.AVEANNAhealth.org/notice-of-data-security-incident.html

135. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class Members (including without limitation Plaintiff Johnson) have suffered actual identity theft and fraud.

136. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class Members have been placed at an imminent, immediate, and continuing increased risk of harm from fraud and identity theft. Defendant inherently recognizes this imminent, immediate, and continuing increased risk because of its acknowledgement that Plaintiffs and Class Members should "regularly monitor credit reports, account statements and benefit statements," and because it offered identity theft protection to Plaintiffs J.A., Johnson, and certain Class Members.

137. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class Members (including without limitation Plaintiff Johnson, as described above) have been forced to expend time dealing with the effects of the Data Breach.

138. Plaintiffs and Class Members have suffered and face substantial risk of out-of-pocket fraud losses such as checking and savings accounts opened in their names (as experienced by Plaintiff Johnson), loans opened in their names, medical services billed in their names, tax return fraud, utility bills opened in their names, credit card fraud, and similar identity theft.

139. Plaintiffs and Class Members face substantial risk of being targeted for future phishing, data intrusion, and other illegal schemes based on their Private

Information as potential fraudsters could use that information to target such schemes more effectively to Plaintiffs and Class Members.

140. Plaintiffs and Class Members may also incur out-of-pocket costs for protective measures such as credit monitoring fees, credit report fees, credit freeze fees, and similar costs directly or indirectly related to the Data Breach.

141. Plaintiffs and Class Members also suffered a loss of value of their Private Information when it was acquired by cyber thieves in the Data Breach. Numerous courts have recognized the propriety of loss of value damages in related cases.

142. Plaintiffs and Class Members were also damaged via benefit-of-the-bargain damages. The express contractual bargain entered into between employee Plaintiffs and employee Class Members included Defendant's contractual obligation to provide adequate data security, which Defendant failed to provide. The patient Plaintiffs and Class Members overpaid for a service that was intended to be accompanied by adequate data security but was not. Part of the price patient Plaintiffs and Class Members paid to Defendant was intended to be used by Defendant to fund adequate security of AVEANNA's computer property and Plaintiffs and Class Members' Private Information and protect Plaintiffs and Class Members' Private Information. Thus, Plaintiffs and the Class Members did not get what they paid for.

143. Plaintiffs and Class Members have spent and will continue to spend significant amounts of time to monitor their financial and medical accounts and records for misuse. Plaintiff Purvis regularly checks a credit monitoring service in which she is enrolled for fraud attempts.

144. Plaintiffs and Class Members have suffered or will suffer actual injury as a direct result of the Data Breach. Many victims suffered ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach relating to:

a. Finding fraudulent charges;

b. Canceling fraudulently created bank accounts;

c. Canceling and reissuing credit and debit cards;

d. Purchasing credit monitoring and identity theft prevention;

e. Addressing their inability to withdraw funds linked to compromised accounts;

f. Taking trips to banks and waiting in line to obtain funds held in limited accounts;

g. Placing “freezes” and “alerts” with credit reporting agencies;

h. Spending time on the phone with or at a financial institution to dispute fraudulent charges;

i. Contacting financial institutions and closing or modifying financial accounts;

j. Resetting automatic billing and payment instructions from compromised credit and debit cards to new ones;

k. Paying late fees and declined payment fees imposed as a result of failed automatic payments that were tied to compromised cards that had to be cancelled; and

l. Closely reviewing and monitoring bank accounts and credit reports for unauthorized activity for years to come.

145. Moreover, Plaintiffs and Class Members have an interest in ensuring that their Private Information, which is believed to remain in the possession of Defendant, is protected from further breaches by the implementation of sufficient security measures and safeguards, including but not limited to, making sure that the storage of data or documents containing personal and financial information is not accessible online and that access to such data is password-protected.

146. Further, as a result of Defendant's conduct, Plaintiffs and Class Members are forced to live with the anxiety that their Private Information—which contains the most intimate details about a person's life, including what ailments they suffer, whether physical or mental—may be disclosed to the entire world, thereby

subjecting them to embarrassment and depriving them of any right to privacy whatsoever.

147. As a direct and proximate result of Defendant's actions and inactions, Plaintiffs and Class Members have suffered a loss of privacy and are at an imminent and increased risk of future harm.

148. Although their PII and PHI was improperly exposed from July 9, 2019 to August 24, 2019, Defendant did not discover the Data Breach until August 24, 2019, and affected patients were not notified of the Data Breach until some time after February 14, 2020, depriving them of the ability to promptly mitigate potential adverse consequences resulting from the Data Breach. As a result of Defendant's delay in detecting and notifying consumers of the Data Breach, the risk of fraud for Plaintiffs and Class Members has been driven even higher.

CLASS ACTION ALLEGATIONS

149. Plaintiffs bring this action on behalf of themselves and on behalf of all other persons similarly situated ("the Class").

150. Plaintiffs propose the following Class definitions, subject to amendment as appropriate:

> All persons who utilized Defendant AVEANNA's services whose Private Information was maintained on Defendant AVEANNA's email and computer system that was compromised in the Data Breach, and who were sent notice of the Data Breach.

> The Employee Subclass: All current and former employees or contractors of AVEANNA whose PII was compromised in the Data Breach that AVEANNA discovered on or about August 24, 2019, and who were sent notice of the Data Breach.

151. Excluded from the Class and Subclass are Defendant's officers and directors; any entity in which Defendant has a controlling interest; and the affiliates, legal representatives, attorneys, successors, heirs, and assigns of Defendant. Excluded also from the Class are members of the judiciary to whom this case is assigned, their families and members of their staff.

152. Numerosity. The Members of the Class are so numerous that joinder of all of them is impracticable. While the exact number of Class Members is unknown to Plaintiffs at this time, based on information and belief, the Class consists of approximately 166,077 patients (and their family members), and unknown number of employees and former employees of Defendant AVEANNA whose data was compromised in the Data Breach.

153. Commonality. There are questions of law and fact common to the Class, which predominate over any questions affecting only individual Class Members. These common questions of law and fact include, without limitation:

a. Whether Defendant unlawfully used, maintained, lost, or disclosed Plaintiffs and Class Members' Private Information;

b. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

c. Whether Defendant's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations including, *e.g.*, HIPAA;

d. Whether Defendant's data security systems prior to and during the Data Breach were consistent with industry standards;

e. Whether Defendant owed a duty to Class Members to safeguard their Private Information;

f. Whether Defendant breached its duty to Class Members to safeguard their Private Information;

g. Whether computer hackers obtained Class Members' Private Information in the Data Breach;

h. Whether Defendant knew or should have known that its data security systems and monitoring processes were deficient;

i. Whether Plaintiffs and Class Members suffered legally cognizable damages as a result of Defendant's misconduct;

j. Whether Defendant's conduct was negligent;

k. Whether Defendant's conduct was *per se* negligent;

l. Whether Defendant's acts, inactions, and practices complained of herein amount to acts of intrusion upon seclusion under the law;

m. Whether Defendant failed to provide notice of the Data Breach in a timely manner; and

n. Whether Plaintiffs and Class Members are entitled to damages, civil penalties, punitive damages, and/or injunctive relief.

154. Typicality. Plaintiffs' claims are typical of those of other Class Members because Plaintiffs' Private Information, like that of every other Class Member, was compromised in the Data Breach.

155. Adequacy of Representation. Plaintiffs will fairly and adequately represent and protect the interests of the Members of the Class. Plaintiffs' Counsel are competent and experienced in litigating class actions.

156. Predominance. Defendant has engaged in a common course of conduct toward Plaintiffs and Class Members, in that all the Plaintiffs and Class Members' Private Information was stored on the same computer systems and unlawfully accessed in the same way. The common issues arising from Defendant's conduct

affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

157. Superiority. A class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a class action, most Class Members would likely find that the cost of litigating their individual claims is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for Defendant. In contrast, the conduct of this action as a class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class Member.

158. Defendant has acted on grounds that apply generally to the Class as a whole, so that class certification, injunctive relief, and corresponding declaratory relief are appropriate on a class-wide basis.

CAUSES OF ACTION

FIRST COUNT

Negligence
(On Behalf of Plaintiffs and All Class Members)

159. Plaintiffs re-allege and incorporate by reference Paragraphs 1 through 158 above as if fully set forth herein.

160. Defendant required Plaintiffs and Class Members to submit non-public Private Information in order to obtain medical services, or as a condition of employment.

161. By collecting and storing this data in its computer property, and sharing it and using it for commercial gain, Defendant had a duty of care to use reasonable means to secure and safeguard its computer property—and Plaintiffs and Class Members' Private Information held within it—to prevent disclosure of the Private Information, and to safeguard the Private Information from theft. Defendant's duty included a responsibility to implement processes by which it could detect a breach of its security systems in a reasonably expeditious period of time and to give prompt notice to those affected in the case of a data breach.

162. Defendant owed a duty of care to Plaintiffs and Class Members to provide data security consistent with industry standards, applicable standards of care from statutory authority like HIPPA and Section 5 of the FTCA, and other

requirements discussed herein, and to ensure that its systems and networks, and the personnel responsible for them, adequately protected the Private Information.

163. Defendant's duty of care to use reasonable security measures arose as a result of the special relationships that existed between Defendant and its client patients, which is recognized by laws and regulations including but not limited to HIPAA, as well as common law, or from the employer-employee relationship. Defendant was in a position to ensure that its systems were sufficient to protect against the foreseeable risk of harm to Class Members from a data breach.

164. Defendant's duty to use reasonable security measures under HIPAA required Defendant to "reasonably protect" confidential data from "any intentional or unintentional use or disclosure" and to "have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information." 45 C.F.R. § 164.530(c)(1). Some or all of the medical information at issue in this case constitutes "protected health information" within the meaning of HIPAA.

165. In addition, Defendant had a duty to employ reasonable security measures under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

166. Defendant's duty to use reasonable care in protecting confidential data arose not only as a result of the statutes and regulations described above, but also because Defendant is bound by industry standards to protect confidential Private Information.

167. Defendant breached its duties, and thus was negligent, by failing to use reasonable measures to protect Plaintiffs and Class Members' Private Information. The specific negligent acts and omissions committed by Defendant include, but are not limited to, the following:

a. Mishandling phishing emails, so as to allow for unauthorized person(s) to access Plaintiffs' and Class Members' Private Information;

b. Failing to adopt, implement, and maintain adequate security measures to safeguard Plaintiffs and Class Members' Private Information;

c. Failing to adequately monitor the security of its networks and systems;

d. Failure to periodically ensure that its email system had plans in place to maintain reasonable data security safeguards;

e. Allowing unauthorized access to Plaintiffs and Class Members' Private Information;

f. Failing to detect in a timely manner that Plaintiffs and Class Members' Private Information had been compromised; and

g. Failing to timely notify Plaintiffs and Class Members about the Data Breach so that they could take appropriate steps to mitigate the potential for identity theft and other damages.

168. It was foreseeable that Defendant's failure to use reasonable measures to protect Plaintiffs and Class Members' Private Information would result in injury to Plaintiffs and Class Members. Further, the breach of security was reasonably foreseeable given the known high frequency of cyberattacks and data breaches in the medical industry.

169. It was therefore foreseeable that the failure to adequately safeguard Plaintiffs and Class Members' Private Information would result in one or more types of injuries to Plaintiffs and Class Members.

170. Plaintiffs and Class Members are entitled to compensatory and consequential damages suffered as a result of the Data Breach

171. Plaintiffs and Class Members are also entitled to injunctive relief requiring Defendant to, *inter alia*: (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) continue to provide adequate credit monitoring to all Class Members.

SECOND COUNT

Intrusion Into Private Affairs / Invasion Of Privacy (On Behalf of Plaintiffs and All Class Members)

172. Plaintiffs repeat and re-allege each and every allegation contained in Paragraphs 1 through 158 as if fully set forth herein.

173. The state of Georgia recognizes the tort of Intrusion into Private Affairs, and adopts the formulation of that tort found in the Restatement (Second) of Torts, which states:

> One who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns, is subject to liability to the other for invasion of his privacy, if the intrusion would be highly offensive to a reasonable person.

Restatement (Second) of Torts § 652B (1977).

174. Plaintiffs and Class Members had a reasonable expectation of privacy in the Private Information Defendant mishandled.

175. Defendant's conduct as alleged above intruded upon Plaintiffs and Class Members' seclusion under common law.

176. By intentionally failing to keep Plaintiffs and Class Members' Private Information safe, and by intentionally misusing and/or disclosing said information to unauthorized parties for unauthorized use, Defendant intentionally invaded Plaintiffs and Class Members' privacy by intentionally and substantially intruding into Plaintiffs and Class Members' private affairs in a manner that identifies

Plaintiffs and Class Members and that would be highly offensive and objectionable to an ordinary person, and by intentionally causing anguish or suffering to Plaintiffs and Class Members.

177. Defendant knew that an ordinary person in Plaintiffs' or a Class Member's position would consider Defendant's intentional actions highly offensive and objectionable.

178. Defendant invaded Plaintiffs and Class Members' right to privacy and intruded into Plaintiffs and Class Members' private affairs by intentionally misusing and/or disclosing their Private Information without their informed, voluntary, affirmative, and clear consent.

179. Defendant intentionally concealed from Plaintiffs and Class Members an incident that misused and/or disclosed their Private information without their informed, voluntary, affirmative, and clear consent.

180. As a proximate result of such intentional misuse and disclosures, Plaintiffs and Class Members' reasonable expectations of privacy in their Private Information was unduly frustrated and thwarted. Defendant's conduct, amounting to a substantial and serious invasion of Plaintiffs and Class Members' protected privacy interests, caused anguish and suffering such that an ordinary person would consider Defendant's intentional actions or inaction highly offensive and objectionable.

181. In failing to protect Plaintiffs and Class Members' Private Information, and in intentionally misusing and/or disclosing their Private Information, Defendant acted with intentional malice and oppression and in conscious disregard of Plaintiffs and Class Members' rights to have such information kept confidential and private. Plaintiffs, therefore, seek an award of damages on behalf of themselves and the Class.

THIRD COUNT

Breach of Express Contract
(On Behalf of Plaintiffs and All Class Members except for the Employee Subclass)

182. Plaintiffs re-allege and incorporate by reference Paragraphs 1 through 158 above as if fully set forth herein.

183. Plaintiffs and Members of the Class allege that they entered into valid and enforceable express contracts, or were third-party beneficiaries of valid and enforceable express contracts, with Defendant for the provision of medical and health care services.

184. Specifically, Plaintiffs entered into a valid and enforceable express contract with Defendant when Plaintiff Purvis first brought Plaintiff J.A. to Defendant for pediatric medical care in 2018.

185. The valid and enforceable express contracts to provide medical and health care services that Plaintiffs and Class Members entered into with Defendant

include Defendant's promise to protect nonpublic Private Information given to Defendant or that Defendant gathers on its own from disclosure.

186. Under these express contracts, Defendant and/or its affiliated healthcare providers, promised and were obligated to: (a) provide healthcare to Plaintiffs and Class Members; and (b) protect Plaintiffs and the Class Members' PII/PHI: (i) provided to obtain such healthcare; and/or (ii) created as a result of providing such healthcare. In exchange, Plaintiffs and Members of the Class agreed to pay money for these services, and to turn over their Private Information.

187. Both the provision of medical services healthcare and the protection of Plaintiffs and Class Members' Private Information were material aspects of these express contracts.

188. The express contracts for the provision of medical services – contracts that include the contractual obligations to maintain the privacy of Plaintiffs and Class Members' Private Information—are formed and embodied in multiple documents, including (among other documents) Defendant's Privacy Notice.

189. At all relevant times, Defendant expressly represented in its Privacy Notice that it would, among other things: (i) "[m]aintain the privacy of protected health information;" (ii) "[p]rovide you with this notice of its legal duties and privacy practices with respect to your protected health information;" (iii) "[n]otify you following a breach of unsecured protected health information;" (iv) [a]bide by the

terms of this notice; and (v) "[o]btain your written authorization to use or disclose your health information for reasons other than those listed above and permitted under law."

190. Defendant's express representations, including, but not limited to, express representations found in its Notice of Privacy Practices, formed and embodied an express contractual obligation requiring Defendant to implement data security adequate to safeguard and protect the privacy of Plaintiffs and Class Members' Private Information.

191. Consumers of healthcare value their privacy, the privacy of their dependents, and the ability to keep their Private Information associated with obtaining healthcare private. To customers such as Plaintiffs and Class Members, healthcare that does not adhere to industry standard data security protocols to protect Private Information is fundamentally less useful and less valuable than healthcare that adheres to industry-standard data security. Plaintiffs and Class Members would not have entered into these contracts with Defendant and/or its affiliated healthcare providers as a direct or third-party beneficiary without an understanding that their Private Information would be safeguarded and protected.

192. A meeting of the minds occurred, as Plaintiffs and Members of the Class agreed to and did provide their Private Information to Defendant and/or its affiliated healthcare providers, and paid for the provided healthcare in exchange for,

amongst other things, both the provision of healthcare and medical services and the protection of their Private Information.

193. Plaintiffs and Class Members performed their obligations under the contract when they paid for their health care services and provided their Private Information.

194. Defendant materially breached its contractual obligation to protect the nonpublic Private Information Defendant gathered when the information was accessed and exfiltrated by unauthorized personnel as part of the Data Breach.

195. Defendant materially breached the terms of these express contracts, including, but not limited to, the terms stated in the relevant Notice of Privacy Practices. Defendant did not maintain the privacy of Plaintiffs and Class Members' Private Information as evidenced by its notifications of the Data Breach to Plaintiffs and approximately 166,077 Class Members. Specifically, Defendant did not comply with industry standards, standards of conduct embodied in statutes like HIPAA and Section 5 of the FTCA, or otherwise protect Plaintiffs and the Class Members' Private Information, as set forth above.

196. The Data Breach was a reasonably foreseeable consequence of Defendant's actions in breach of these contracts.

197. As a result of Defendant's failure to fulfill the data security protections promised in these contracts, Plaintiffs and Members of the Class did not receive the

full benefit of the bargain, and instead received healthcare and other services that were of a diminished value to that described in the contracts. Plaintiffs and Class Members therefore were damaged in an amount at least equal to the difference in the value of the healthcare with data security protection they paid for and the healthcare they received.

198. Had Defendant disclosed that its security was inadequate or that it did not adhere to industry-standard security measures, neither the Plaintiffs, the Class Members, nor any reasonable person would have purchased healthcare from Defendant and/or its affiliated healthcare providers.

199. As a direct and proximate result of the Data Breach, Plaintiffs and Class Members have been harmed and have suffered, and will continue to suffer, actual damages and injuries, including without limitation the release, disclosure, and publication of their Private Information, the loss of control of their Private Information, the imminent risk of suffering additional damages in the future, disruption of their medical care and treatment, out-of-pocket expenses, and the loss of the benefit of the bargain they had struck with Defendant.

200. Plaintiffs and Class Members are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

FOURTH COUNT

Breach of Implied Contract
(On Behalf of Plaintiffs and All Class Members)

201. Plaintiffs re-allege and incorporate by reference Paragraphs 1 through 158 above as if fully set forth herein.

202. When Plaintiffs and Class Members provided their Private Information to AVEANNA in exchange for Defendant's services, or as a condition of employment, they entered into implied contracts with Defendant pursuant to which Defendant agreed to reasonably protect such Private Information.

203. Defendant solicited and invited Class Members to provide their Private Information as part of Defendant's regular business practices. Plaintiffs and Class Members accepted Defendant's offers and provided their Private Information to Defendant.

204. Members of the Employee Subclass (including Plaintiff Johnson) also provided their labor and employee services to Defendant, in addition to turning over their PII, in exchange for Defendant's promise to protect their PII from unauthorized disclosure.

205. Defendant AVEANNA manifested its intent to enter into an implied contract that included a contractual obligation to reasonably protect Plaintiffs and Class Members' Private Information through, among other things, its Privacy Notice.

206. In entering into such implied contracts, Plaintiffs and Class Members reasonably believed and expected that Defendant's data security practices complied with relevant laws and regulations, including HIPAA, and were consistent with industry standards.

207. Class Members who paid money to Defendant reasonably believed and expected that Defendant would use part of those funds to obtain adequate data security. Defendant failed to do so.

208. Plaintiffs and Class Members would not have entrusted their Private Information to Defendant in the absence of the implied contracts between them and Defendant to keep their information reasonably secure. Plaintiffs and Class Members would not have entrusted their Private Information to Defendant in the absence of its implied promise to monitor its computer systems and networks to ensure that it adopted reasonable data security measures.

209. Plaintiffs and Class Members fully and adequately performed their obligations under the implied contracts with Defendant.

210. Defendant breached its implied contracts with Plaintiffs and Class Members by failing to safeguard and protect their Private Information.

211. As a result of Defendant's failure to fulfill the data security protections promised in these implied contracts, Plaintiffs and Members of the Class did not receive the full benefit of the bargain, and instead received healthcare and other

services that were of a diminished value to that agreed upon in the implied contracts. Plaintiffs and Class Members therefore were damaged in an amount at least equal to the difference in the value of the healthcare with data security protection they paid for and the healthcare they received.

212. Had Defendant disclosed that its security was inadequate or that it did not adhere to industry-standard security measures, neither the Plaintiffs, the Class Members, nor any reasonable person would have purchased healthcare from Defendant and/or its affiliated healthcare providers.

213. Plaintiffs and Class Members are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

214. Plaintiffs and Class Members are also entitled to injunctive relief requiring Defendant to, *inter alia*: (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide adequate credit monitoring to all Class Members.

FIFTH COUNT

Negligence *Per Se*
(On Behalf of Plaintiffs and All Class Members)

215. Plaintiffs re-allege and incorporate by reference Paragraphs 1 through 158 above as if fully set forth herein.

216. Pursuant to Section 5 of the Federal Trade Commission Act (15 U.S.C.

§ 45), Defendant had a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiffs and Class Members' Private Information.

217. Plaintiffs and Class Members are within the class of persons that the FTCA was intended to protect.

218. The harm that occurred as a result of the Data Breach is the type of harm the FTCA was intended to guard against. The FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiffs and the Class.

219. Pursuant to HIPAA (42 U.S.C. § 1302d, *et seq.*), Defendant had a duty to implement reasonable safeguards to protect Plaintiffs and Class Members' Private Information.

220. Pursuant to HIPAA, Defendant had a duty to render the electronic PHI it maintained unusable, unreadable, or indecipherable to unauthorized individuals, as specified in the HIPAA Security Rule by "the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key" (45 C.F.R. § 164.304 definition of encryption).

221. Plaintiffs and Class Members are within the class of persons that the HIPAA was intended to protect.

222. The harm that occurred as a result of the Data Breach is the type of harm that HIPAA was intended to guard against. The Federal Health and Human Services' Office for Civil Rights ("OCR") has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures relating to protected health information, caused the same harm as that suffered by Plaintiffs and the Class.

223. Defendant breached its duties to Plaintiffs and Class Members under the Federal Trade Commission Act and HIPAA, by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiffs and Class Members' Private Information.

224. Defendant's failure to comply with applicable laws and regulations constitutes negligence *per se*.

225. But for Defendant's wrongful and negligent breach of its duties owed to Plaintiffs and Class Members, Plaintiffs and Class Members would not have been injured.

226. The injury and harm suffered by Plaintiffs and Class Members was the reasonably foreseeable result of Defendant's breach of its duties. Defendant knew or should have known that it was failing to meet its duties, and that Defendant's breach would cause Plaintiffs and Class Members to experience the foreseeable harms associated with the exposure of their Private Information.

227. As a direct and proximate result of Defendant's negligent conduct, Plaintiffs and Class Members have suffered injury and are entitled to compensatory, consequential, and punitive damages in an amount to be proven at trial.

SIXTH COUNT

Breach of Fiduciary Duty
(On Behalf of Plaintiffs and All Class Members)

228. Plaintiffs re-allege and incorporate by reference Paragraphs 1 through 158 above as if fully set forth herein.

229. In light of the special relationships between Defendant and Plaintiffs and Class Members, whereby Defendant became guardians of Plaintiffs and Class Members' Private Information, Defendant became a fiduciary by its undertaking and guardianship of the Private Information, to act primarily for the benefit of its patients, including Plaintiffs and Class Members: (i) for the safeguarding of Plaintiffs and Class Members' Private Information; (ii) to timely notify Plaintiffs and Class Members of a data breach and disclosure; and (iii) maintain complete and accurate records of what Private Information (and where) Defendant did and does store.

230. Defendant has a fiduciary duty to act for the benefit of Plaintiffs and Class Members upon matters within the scope of its patients' relationship, in particular, to keep secure the Private Information of its patients.

231. Defendant has a fiduciary duty to act for the benefit of the members of the Employee Subclass upon matters within the scope of its employer-employee relationship, to keep secure the PII of its employees.

232. Defendant breached its fiduciary duties to Plaintiffs and Class Members by failing to diligently discovery, investigate, and give notice of the Data Breach in a reasonable and practicable period of time.

233. Defendant breached its fiduciary duties to Plaintiffs and Class Members by failing to encrypt and otherwise protect the integrity of the systems containing Plaintiffs and Class Members' Private Information.

234. Defendant breached its fiduciary duties owed to Plaintiffs and Class Members by failing to timely notify and/or warn Plaintiffs and Class Members of the Data Breach.

235. Defendant breached its fiduciary duties owed to Plaintiffs and Class Members by failing to ensure the confidentiality and integrity of electronic PHI Defendant created, received, maintained, and transmitted, in violation of 45 C.F.R. § 164.306(a)(1).

236. Defendant breached its fiduciary duties owed to Plaintiffs and Class Members by failing to implement technical policies and procedures for electronic information systems that maintain electronic PHI to allow access only to those

persons or software programs that have been granted access rights in violation of 45 C.F.R. § 164.312(a)(1).

237. Defendant breached its fiduciary duties owed to Plaintiffs and Class Members by failing to implement policies and procedures to prevent, detect, contain, and correct security violations, in violation of 45 C.F.R. § 164.308(a)(1).

238. Defendant breached its fiduciary duties owed to Plaintiffs and Class Members by failing to identify and respond to suspected or known security incidents and to mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity in violation of 45 C.F.R. § 164.308(a)(6)(ii).

239. Defendant breached its fiduciary duties owed to Plaintiffs and Class Members by failing to protect against any reasonably anticipated threats or hazards to the security or integrity of electronic PHI in violation of 45 C.F.R. § 164.306(a)(2).

240. Defendant breached its fiduciary duties owed to Plaintiffs and Class Members by failing to protect against any reasonably anticipated uses or disclosures of electronic PHI that are not permitted under the privacy rules regarding individually identifiable health information in violation of 45 C.F.R. § 164.306(a)(3).

241. Defendant breached its fiduciary duties owed to Plaintiffs and Class Members by failing to ensure compliance with the HIPAA security standard rules by its workforce in violation of 45 C.F.R. § 164.306(a)(94).

242. Defendant breached its fiduciary duties owed to Plaintiffs and Class Members by impermissibly and improperly using and disclosing PHI that is and remains accessible to unauthorized person(s) in violation of 45 C.F.R. § 164.502, et seq.

243. Defendant breached its fiduciary duties owed to Plaintiffs and Class Members by failing to effectively train all members of its workforce (including independent contractors) on the policies and procedures with respect to PHI as necessary and appropriate for the members of its workforce to carry out their functions and to maintain security of PHI in violation of 45 C.F.R. § 164.530(b) and 45 C.F.R. § 164.308(a)(5).

244. Defendant breached its fiduciary duties owed to Plaintiffs and Class Members by failing to design, implement, and enforce policies and procedures establishing physical and administrative safeguards to reasonably safeguard PHI, in compliance with 45 C.F.R. § 164.530(c).

245. Defendant breached its fiduciary duties to Plaintiffs and Class Members by otherwise failing to safeguard Plaintiffs and Class Members' Private Information.

246. As a direct and proximate result of Defendant's breaches of its fiduciary duties, Plaintiffs and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the compromise, publication, and/or theft of their Private Information; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of their Private Information; (iv) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (v) the continued risk to their Private Information, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information in its continued possession; (vi) future costs in terms of time, effort, and money that will be expended as result of the Data Breach for the remainder of the lives of Plaintiffs and Class Members; and (vii) the diminished value of Defendant's services they received.

247. As a direct and proximate result of Defendant's breaches of its fiduciary duties, Plaintiffs and Class Members have suffered and will continue to suffer other forms of injury and/or harm, and other economic and non-economic losses.

SEVENTH COUNT

Breach of Confidence
(On Behalf of Plaintiffs and All Class Members)

248. Plaintiffs re-allege and incorporate by reference Paragraphs 1 through 158 above as if fully set forth herein.

249. At all times during Plaintiffs and Class Members' interactions with Defendant, Defendant was fully aware of the confidential and sensitive nature of Plaintiffs and Class Members' Private Information that Plaintiffs and Class Members provided to Defendant.

250. As alleged herein and above, Defendant's relationship with Plaintiffs and Class Members was governed by terms and expectations that Plaintiffs and Class Members' Private Information would be collected, stored, and protected in confidence, and would not be disclosed the unauthorized third parties.

251. Plaintiffs and Class Members provided their respective Private Information to Defendant with the explicit and implicit understandings that Defendant would protect and not permit the Private Information to be disseminated to any unauthorized parties.

252. Plaintiffs and Class Members also provided their Private Information to Defendant with the explicit and implicit understandings that Defendant would take precautions to protect that Private Information from unauthorized disclosure,

such as following basic principles of protecting its networks and data systems, including employees' email accounts.

253. Defendant voluntarily received in confidence Plaintiffs and Class Members' Private Information with the understanding that Private Information would not be disclosed or disseminated to the public or any unauthorized third parties.

254. Due to Defendant's failure to prevent, detect, avoid the Data Breach from occurring by, *inter alia*, following best information security practices to secure Plaintiffs and Class Members' Private Information, Plaintiffs and Class Members' Private Information was disclosed and misappropriated to unauthorized third parties beyond Plaintiffs and Class Members' confidence, and without their express permission.

255. As a direct and proximate cause of Defendant's actions and/or omissions, Plaintiffs and Class Members have suffered damages.

256. But for Defendant's disclosure of Plaintiffs and Class Members' Private Information in violation of the parties' understanding of confidence, their Private Information would not have been compromised, stolen, viewed, accessed, and used by unauthorized third parties. Defendant's Data Breach was the direct and legal cause of the theft of Plaintiffs and Class Members' Private Information, as well as the resulting damages.

257. The injury and harm Plaintiffs and Class Members suffered was the reasonably foreseeable result of Defendant's unauthorized disclosure of Plaintiffs and Class Members' Private Information. Defendant knew its computer systems and technologies for accepting and securing Plaintiffs and Class Members' Private Information had numerous security vulnerabilities.

258. As a direct and proximate result of Defendant's breaches of confidence, Plaintiffs and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the compromise, publication, and/or theft of their Private Information; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of their Private Information; (iv) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (v) the continued risk to their Private Information, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information in its continued possession; (vi) future costs in terms of time, effort, and money that will be expended as result of the Data Breach for the remainder of the lives of

Plaintiffs and Class Members; and (vii) the diminished value of Defendant's services they received.

259. As a direct and proximate result of Defendant's breaches of its fiduciary duties, Plaintiffs and Class Members have suffered and will continue to suffer other forms of injury and/or harm, and other economic and non-economic losses.

EIGHTH COUNT

Breach of Express Contract
(On Behalf of Plaintiff Johnson and the Employee Subclass)

260. Plaintiffs re-allege and incorporate by reference Paragraphs 1 through 158 above as if fully set forth herein.

261. Plaintiff Johnson and Members of the Employee Subclass allege that they entered into valid and enforceable express employment contracts with Defendant.

262. Specifically, Plaintiff Johnson entered into a valid and enforceable express employment contract with Defendant, working first as an IEP aide and later as a substitute teacher.

263. The valid and enforceable express employment contracts that Plaintiff Johnson and Employee Subclass Members entered into with Defendant included Defendant's promise to protect nonpublic Private Information given to Defendant or that Defendant gathers on its own from disclosure.

264. Under these express contracts, Defendant promised and was obligated to protect Plaintiff Johnson's and the Employee Subclass Members' PII. In exchange, Plaintiff Johnson and Members of the Employee Subclass agreed to provide Defendant with their labor and services, and to turn over their Private Information.

265. The protection of Plaintiff Johnson's and Employee Subclass Members' Private Information was a material aspect of the express employment contracts.

266. Employees value their privacy, the privacy of their dependents, and the ability to keep their Private Information associated with their employment private. Plaintiff Johnson and Employee Subclass Members would not have entered into their employment contracts with Defendant without an understanding that their Private Information would be safeguarded and protected, and a further understanding that Defendant would adhere to industry standard data security protocols.

267. A meeting of the minds occurred, as Plaintiff Johnson and Members of the Employee Subclass agreed to and did provide their Private Information to Defendant, and provided their labor and services, in exchange for both compensation and wages and for the protection of their Private Information.

268. Plaintiff Johnson and Members of the Employee Subclass performed their obligations under the contract when they provided their labor and services and provided their Private Information to Defendant.

269. Defendant materially breached its contractual obligation to protect the nonpublic Private Information Defendant gathered when the information was accessed and exfiltrated by unauthorized personnel as part of the Data Breach.

270. Defendant materially breached the terms of these express contracts. Defendant did not maintain the privacy of Plaintiff Johnson's and Employee Subclass Members' Private Information as evidenced by its notifications of the Data Breach to Plaintiff Johnson and at least 166,077 Employee Subclass Members. Specifically, Defendant did not comply with industry standards, standards of conduct embodied in statutes like Section 5 of the FTCA, or otherwise protect Plaintiff Johnson's and the Employee Subclass Members' Private Information, as set forth above.

271. The Data Breach was a reasonably foreseeable consequence of Defendant's actions in breach of these contracts.

272. As a result of Defendant's failure to fulfill the data security protections promised in these contracts, Plaintiff Johnson and Members of the Employee Subclass did not receive the full benefit of their bargain. Plaintiff and Employee Subclass Members therefore were damaged in an amount at least equal to the

difference in the value of the employment with data security protection for which they contracted and that which they actually received.

273. Had Defendant disclosed that its security was inadequate or that it did not adhere to industry-standard security measures, neither Plaintiff Johnson, the Employee Subclass Members, nor any reasonable person would have agreed to be employed by Defendant.

274. As a direct and proximate result of the Data Breach, Plaintiff Johnson and the Employee Subclass Members have been harmed and have suffered, and will continue to suffer, actual damages and injuries, including without limitation identity theft and fraud, the release, disclosure, and publication of their Private Information, the loss of control of their Private Information, the imminent risk of suffering additional damages in the future, out-of-pocket expenses, and the loss of the benefit of the bargain they had struck with Defendant.

275. Plaintiff Johnson and Employee Subclass Members are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs pray for judgment as follows:

a) For an Order certifying this action as a Class action and appointing Plaintiffs and their counsel to represent the Class;

b) For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiffs and Class Members' Private Information, and from refusing to issue prompt, complete and accurate disclosures to Plaintiffs and Class Members;

c) For equitable relief compelling Defendant to utilize appropriate methods and policies with respect to consumer data collection, storage, and safety, and to disclose with specificity the type of PII and PHI (*i.e.*, Private Information) compromised during the Data Breach;

d) For equitable relief requiring restitution and disgorgement of the revenues wrongfully retained as a result of Defendant's wrongful conduct;

e) For an award of actual damages, compensatory damages, and nominal damages, in an amount to be determined, as allowable by law;

f) For an award of punitive damages, as allowable by law;

g) For an award of attorneys' fees and costs, and any other expense, including expert witness fees;

h) Pre- and post-judgment interest on any amounts awarded; and

i) Such other and further relief as this court may deem just and proper.

JURY TRIAL DEMANDED

Plaintiffs demand a trial by jury on all claims so triable.

Dated: August 20, 2020

Respectfully submitted,

/s/ Shireen Hormozdi
Shireen Hormozdi
HORMOZDI LAW FIRM, LLC
1770 Indian Trial Lilburn Road, Suite 175
Norcross, GA 30093
Phone: (678) 395-7795
Fax: (866) 929-2434
shireen@norcrosslawfirm.com

MASON LIETZ & KLINGER LLP
Gary E. Mason (admitted *pro hac vice*)
David K. Lietz (admitted *pro hac vice*)
5101 Wisconsin Avenue NW, Suite 305
Washington, DC 20016
Phone: (202) 429-2290
Fax: (202) 429-2294
gmason@masonllp.com
dlietz@masonllp.com

Gary M. Klinger (admitted *pro hac vice*)
MASON LIETZ & KLINGER LLP
227 W. Monroe Street, Suite 2100
Chicago, IL 60606
Phone: (202) 975-0477
gklinger@masonllp.com

Attorneys for Plaintiffs and the Proposed Classes